UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/815,454	03/31/2004	David Wheeler	884.B58US1	6377

21186 7590 12/11/2007

SCHWEGMAN, LUNDBERG & WOESSNER, P.A.
P.O. BOX 2938
MINNEAPOLIS, MN 55402

EXAMINER	
SHAIFER HARRIMAN, DANT B	
ART UNIT	PAPER NUMBER
2134	
MAIL DATE	DELIVERY MODE
12/11/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/815,454	WHEELER ET AL.	
	Examiner	Art Unit	
	Dant B. Shaifer - Harriman	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03/31/2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1 - 29* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1 - 29* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *31 March 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *05/23/2005, 12/06/2005*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Specification

1. The disclosure is objected to because of the following informalities: the applicant's summary is missing.

Appropriate correction is required.

2. The disclosure is objected to because of the following informalities: in applicant's specification, particularly in section titled, "Related Applicant," the application entitled "Method and Apparatus for a trust processor", this applications serial or application number is not disclosed; the serial number must be disclosed.

Appropriate correction is required.

Claim Rejections - 35 USC § 101

3. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claim(s) 1 – 5 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The claims lack the necessary physical articles or objects to constitute a machine or a manufacture within the meaning of 35 USC 101. They are clearly not a series of steps or acts to be a process nor are they a combination of chemical compounds to be a composition of matter. As such, they fail to fall within a statutory category. They are, at best, functional descriptive material *per se*. Furthermore the examiner would like to note that the claim limitations describe software per se, which is clearly not a statutory category.

Claim(s) 9 – 12 & 16 – 18 & 23 – 25 & 26 – 29 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claims(s) 9 – 12 & 16 – 18 & 23 – 25 &

26 – 29 are directed to cryptographic processor, that contains a non-volatile memory, program instructions, a controller.

This claimed subject matter lacks a practical application of a judicial exception (law of nature, abstract idea, naturally occurring phenomenon) since it fails to produce a useful, concrete and tangible result. Specifically, the claimed subject matter does not produce a tangible result because the claimed subject matter fails to produce a result that is limited to having real world value rather than a result that may be interpreted to be abstract in nature as, for example, a thought, a computation, or manipulated data. More specifically, the claimed subject matter provides for the above mentioned claims recite claim limitations that are conditional in nature, meaning that "if event (Z) happens then event (X) will be executed." Then what if event (Z) doesn't happen, then event (X) will not happen. The examiner point is, if

event (Z) doesn't happen, then nothing **tangible** is happening to event (X), which would be "executing event (X)." Specifically, the examiner notes that the independent claim # 9 is only tangible if the "response is correct", then the examiner concludes that the cryptographic key is just sitting in memory (non - volatile), being **not tangible**.

This produced result remains in the abstract and, thus, fails to achieve the required status of having real world value.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the

applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claim(s) 1 - 5 are rejected under 35 U.S.C. 102(e) as being taught by Kaplan et al. (US Patent # 6704871 B1)

Kaplan teaches:

Claim #1. An apparatus comprising:

- one or more cryptographic units (Col. 6, lines 55 – 61 & Col. 4, lines 42 - 44 & Col. 4, lines 57 - 63); and

- a memory to store one or more data encryption keys and an associated header for the one or more data encryption keys(Col. 6, lines 40 - 45),

wherein

- the associated header defines which of the one or more cryptographic units are to use the data encryption key(Col. 41, lines 53 – 67 & Col. 42, lines 1 – 5).

Claim #2. The apparatus of claim 1, wherein

- the associated header defines a usage type for the data encryption key(Col. 41, lines 53 – 67 & Col. 42, lines 1 – 5).

Claim #3. The apparatus of claim 2 further comprising

- a controller to restrict which of the one more cryptographic units are to use the data encryption key and a type of operation based on the associated header for the data

encryption key(Col. 22, lines 18 – 39 & Col. 24, lines 61 – 65 & Col. 27, lines 56 – 64).

Claim #4. The apparatus of claim 1, wherein

- the associated header defines an identification of a key encryption key used to encrypt the one or more data encryption keys(Col. 7, lines 66 – 67 & Col. 8, lines 1 – 17 & Col. 39, lines 49 – 60 & Col. 40, lines 14 - 20).

Claim #5. The apparatus of claim 1, wherein

- the one or more cryptographic units is from a group consisting of an
- advanced encryption standard unit(),
- a data encryption standard unit(Col. 5, lines 13 - 65),
- a message digest unit() and

- a secure hash algorithm unit(Col. 5, lines 66 - 67 & Col. 6, lines 1 – 5 & Col. 6, lines 61 – 67 & Col. 10, lines 27 - 34) or
- an exponential algorithmic unit().

Claim(s) 6 - 22 are rejected under 35 U.S.C. 102(e) as being taught by Dariel (US Patent # 7058818).

Dariel teaches:

Claim #6. An apparatus comprising:

- a cryptographic processor within a wireless device(Col. 6, lines 4 - 15),

the cryptographic processor comprising:

- a first cryptographic unit to generate an intermediate result from execution of a first operation(Col. 4, lines 19 – 25 & Col. 3, lines 1 – 55 & Col. 3, lines 19 – 25 & Col. 6, lines 14

– 27, Figure # , the examiner notes that the examiner considers the first cryptographic unit as equal to the second cryptographic unit, reasoning that applicant doesn't differentiate between first and second cryptographic unit, therefore they are one and the same); and

- a second cryptographic unit to generate a final result from execution of a second operation based on the intermediate result(Col. 4, lines 19 – 25 & Col. 3, lines 1 – 55 & Col. 3, lines 19 – 25 & Col. 6, lines 14 – 27, Figure # , the examiner notes that the examiner considers the first cryptographic unit as equal to the second cryptographic unit, reasoning that applicant doesn't differentiate between first and second cryptographic unit, therefore they are one and the same),

wherein

- the intermediate result is not accessible external to the cryptographic processor(Col. 4, lines 50 - 52).

Claim #7. The apparatus of claim 6, wherein

- the first cryptographic unit and the second cryptographic unit are from a group consisting of an advanced encryption standard unit, a data encryption standard unit, a message digest unit and a secure hash algorithm unit or an exponential algorithmic unit(Col. 6, lines 55 – 61 & Col. 4, lines 1- 5 & Col. 7, lines 42 - 47).

Claim #8. The apparatus of claim 6, wherein

- the first operation includes the use of a cryptographic key(Col. 3, lines 38 - 47),

wherein

- the cryptographic key is not loaded into the first cryptographic unit until the cryptographic key is authenticated(Col. 3, lines 63 - 67).

Claim #9. A system comprising

- a dipole antenna to receive a communication(Col. 6, lines 4 – 15, the examiner notes that a mobile or cellular phone will have a dipole antenna, that receives radio waves);

- an application processor to generate a primitive instruction for a cryptographic operation that is to use a cryptographic key based on the communication(Col. 4, lines 19 – 25 & Col. 3, lines 1 – 55 & Col. 3, lines 19 – 25 & Col. 6, lines 14 – 27, the examiner considers the co-processor as a application processor that executes encryption and decryption of the data and keys); and

a cryptographic processor that comprises:

- a memory to store the cryptographic key(Col. 6, lines 22 – 29);

a number of cryptographic units, wherein

- one of the number of cryptographic units is to generate a challenge to the use of the cryptographic key, wherein the application processor is to generate a response to the challenge(Col. 3, lines 63 - 67); and

- a controller to load the cryptographic key into one of the number of cryptographic units for execution of the cryptographic operation if the response is correct (Col. 7, lines 20 - 32).

Claim #10. The system of claim 9, wherein

- the cryptographic processor further comprises a nonvolatile memory that is to store a number of microcode instructions(Col. 6, lines 22 – 29),

wherein

- the controller is to load the cryptographic key into one of the number of cryptographic units based on at least part of the number of microcode instructions(Col. 7, lines 20 – 32 &Col. 6, lines 22 – 29).

Claim #11. The system of claim 9, wherein

- the controller is to abort execution of the cryptographic operation if the response is not correct(Col. 7, lines 20 – 32, the examiner notes that to one of ordinary skill in the art, if the user or remote platform isn't authenticated then the request encrypted data will not be transferred).

Claim #12. The system of claim 9, wherein

- the response includes a hash of a password associated with the cryptographic key(Col. 6, lines 55 - 60).

Claim #13. A system comprising:

- an application processor, within a wireless device, to generate a primitive instruction related to a cryptographic operation (Col. 4, lines 19 – 25 & Col. 3, lines 1 – 55 & Col. 3, lines 19 – 25 & Col. 6, lines 14 – 27, the examiner considers the co-processor as a application processor that executes encryption and decryption of the data and keys); and

a cryptographic processor, within the wireless device, the cryptographic processor comprising:

- a controller to receive the primitive instruction, wherein the controller is to retrieve a number of microcode instructions from a nonvolatile memory within the cryptographic

processor (Col. 6, lines 22 – 29 & Col. 7, lines 20 – 32);

- a first functional unit to generate an intermediate result from execution of a first operation based on a first of the number of microcode instructions(Col. 4, lines 19 – 25 & Col. 3, lines 1 – 55 & Col. 3, lines 19 – 25 & Col. 6, lines 14 – 27, Figure # , the examiner notes that the examiner considers the first cryptographic unit as equal to the second cryptographic unit, reasoning that applicant doesn't differentiate between first and second cryptographic unit, therefore they are one and the same); and

- a second functional unit to generate a final result for the cryptographic operation based on the intermediate result, from execution of a second operation based on a second of

the number of microcode instructions, wherein the intermediate result is not accessible external to the cryptographic processor(Col. 4, lines 19 – 25 & Col. 3, lines 1 – 55 & Col. 3, lines 19 – 25 & Col. 6, lines 14 – 27, Figure # , the examiner notes that the examiner considers the first cryptographic unit as equal to the second cryptographic unit, reasoning that applicant doesn't differentiate between first and second cryptographic unit, therefore they are one and the same).

Claim #14. The system of claim 13, wherein

- the cryptographic processor further compromises a volatile memory to store a cryptographic key(Col. 6, lines 22 – 29).

Claim #15. The system of claim 14, wherein

- the second functional unit is to use the cryptographic key to generate the final result, wherein the controller is not to load the cryptographic key into the second functional unit until the application processor is to authenticate the cryptographic key(Col. 3, lines 63 - 67).

Claim #16. A method comprising:

- receiving a primitive instruction into a cryptographic processor(Col. 3, lines 63 - 67, the examiner notes that the cryptographic processor located on the ASIC (application specific integrated circuit) initiates with the content server for requesting content), for

- execution of a cryptographic operation that uses a data encryption key that is protected within the cryptographic processor(Col. 3, lines 25 - 62 & Col. 7, lines 20 - 48);

- retrieving the data encryption key and an associated header for the data encryption key, wherein the associated header defines which of one or more cryptographic units are to use the data encryption key(Col. 3, lines 25 - 62 & Col. 7, lines 20 – 48, the examiner notes that the data packets sent from the content server to the ASIC and cryptographic, co-

processors, will contain the necessary IP addresses to reach the ASIC and processor); and

- performing an operation within one of the one or more cryptographic units using the data encryption key, if the associated header defines the one of the one or more cryptographic units(Col. 3, lines 25 - 62 & Col. 7, lines 20 - 48).

Claim #17. The method of claim 16, wherein

- the associated header defines a usage type for the data encryption key(Col. 3, lines 25 - 62 & Col. 7, lines 20 – 48, the examiner notes that the data packets sent from the content server to the ASIC and cryptographic, co-

processors, will contain the necessary IP addresses to reach the ASIC and processor).

Claim #18. The method of claim 17, wherein

- performing the operation within one of the one or more cryptographic units using the data encryption key comprises performing the operation within one of the one or more cryptographic units using the data encryption key if a type of the operation is defined by the usage type(Col. 3, lines 25 - 62 & Col. 7, lines 20 – 48, the examiner notes that the data packets sent from the content server to the ASIC and cryptographic, co-processors, will contain the necessary IP addresses to reach the ASIC and processor).

Claim #19. A method comprising:

- receiving a primitive instruction into a cryptographic processor from an application executing on an application processor, for execution of a cryptographic operation that uses a cryptographic key that is protected within the cryptographic processor (Col. 3, lines 63 – 67 & Col. 7, lines 20 – 48);

- generating a challenge for use of the cryptographic key back to the application (Col. 3, lines 63 – 67 & Col. 7, lines 20 – 48, the examiner notes that the user platform or remote

platform send a authorization request or challenge to obtain clearance to gain access to the request content from the content server);

- receiving a response to the challenge into the cryptographic processor from the application (Col. 3, lines 63 – 67 & Col. 7, lines 20 – 48, the examiner notes that the user platform or remote platform “will” or “will not" have access to the requested content based on if the user's authentication data matches the content server user's authentication data);

performing the following operations, if the response is correct:

- loading the cryptographic key into a functional unit of the cryptographic processor (Col. 3, lines 63 – 67 & Col. 7, lines

20 – 48); and

- executing an operation within the functional unit using the cryptographic key (Col. 3, lines 63 – 67 & Col. 7, lines 20 – 48).

Claim #20. The method of claim 19, further comprising

- aborting execution of the primitive instruction if the response is not correct (Col. 3, lines 63 – 67 & Col. 7, lines 20 – 48, the examiner notes that the user platform or remote platform "will" or "will not" have access to the requested content based on if the user's authentication data matches the content server user's authentication data).

Claim #21. The method of claim 19, wherein

- receiving the response to the challenge into the cryptographic processor from the application includes receiving a hash of a password associated with the cryptographic key (Col. 3, lines 63 – 67 & Col. 7, lines 20 – 48).

Claim #22. The method of claim 21, wherein

- performing the following operations, if the response is correct comprises performing the following operations, if the hash of the password is equal to a hash of the password generated within the cryptographic processor (Col. 3, lines

63 – 67 & Col. 7, lines 20 – 48).

Claim(s) 23-29 are rejected under 35 U.S.C. 102(e) as being taught by Howard et al. (US Patent # 7269736 B2).

Howard teaches:

Claim #23. A machine-readable medium that provides instructions, which when executed by a machine, cause said machine to perform operations comprising (Col. 3, lines 9 - 13):

- receiving a primitive instruction into a cryptographic processor, for execution of a cryptographic operation that uses a data encryption key that is protected within the cryptographic processor (Col. 2, lines 60 – 65 & Col. 5, lines

17 - 22);

- retrieving the data encryption key and an associated header for the data encryption key, wherein the associated header defines which of one or more cryptographic units are to use the data encryption key(Col. 2, lines 60 – 65 & Col. 5, lines 17 – 49 & Figure # 2a & 2b, the examiner notes that the data packets that are sent to the second device will inherently have a source and destination address to the processor of the mobile device, to be encrypted); and

- performing an operation within one of the one or more cryptographic units using the data encryption key, if the associated header defines the one of the one or more cryptographic units (Col. 2, lines 60 – 65 & Col. 5, lines 17 -

49).

Claim #24. The machine-readable medium of claim 23, wherein

- the associated header defines a usage type for the data encryption key (Col. 2, lines 60 – 65 & Col. 5, lines 17 – 49, the examiner notes that the data packets will indicate whether they are to be encrypted or not to the second device).

Claim #25. The machine-readable medium of claim 24, wherein

- performing the operation within one of the one or more cryptographic units using the data encryption key comprises

performing the operation within one of the one or more cryptographic units using the data encryption key if a type of the operation is defined by the usage type (Col. 2, lines 60 – 65 & Col. 5, lines 17 – 49 & Figure # 2a & 2b, the examiner notes that the data packets that are sent to the second device will inherently have a source and destination address to the processor of the mobile device, to be encrypted).

Claim #26. A machine-readable medium that provides instructions, which when executed by a machine, cause said machine to perform operations comprising (Col. 3, lines 9 - 13):

- receiving a primitive instruction into a cryptographic processor from an application executing on an application processor, for execution of a cryptographic operation that

uses a cryptographic key that is protected within the cryptographic processor (Col. 5, lines 17 - 22);

- generating a challenge for use of the cryptographic key back to the application(Col. 6, lines 15 - 18);

- receiving a response to the challenge into the cryptographic processor from the application(Col. 6, lines 15 - 18);

performing the following operations, if the response is correct:

- loading the cryptographic key into a functional unit of the cryptographic processor (Figure # 2 & Col. 5, lines 16 - 40); and

- executing an operation within the functional unit using the cryptographic key(Col. 5, lines 16 - 40).

Claim #27. The machine-readable medium of claim 26, further comprising

- aborting execution of the primitive instruction if the response is not correct(Col. 6, lines 15 – 18, the examiner notes that if the user cancels the transfer of the data to be encrypted the execution will be “aborted”).

Claim #28. The machine-readable medium of claim 26, wherein

- receiving the response to the challenge into the cryptographic processor from the application includes receiving a hash of a password associated with the

cryptographic key(Col. 6, lines 15 – 18).

Claim # 29. The machine-readable medium of claim 28, wherein

- performing the following operations, if the response is correct comprises performing the following operations, if the hash of the password is equal to a hash of the password generated within the cryptographic processor (Col. 6, lines 15 – 18).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Dant B. Shaifer - Harriman whose telephone number is 571-272-7910. The examiner can normally be reached on Monday - Thursday: 8:00am - 5:30pm Alt.Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

D. S. H.

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

12/7/07